**CloudArmor: Supporting Reputation-based Trust Management for Cloud Services**

**ABSTRACT:**

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers’ privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments. In this article, we describe the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks and preserve users’ privacy, ii) an adaptive and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to compare the trustworthiness of cloud services, and iii) an availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services.

**EXISTING SYSTEM:**

According to researchers at Berkeley, trust and security are ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs). Consumers’ feedback is a good source to assess the overall trustworthiness of cloud services. Several researchers have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Guaranteeing the availability of TMS is a difficult problem due to the unpredictable number of users and the highly dynamic nature of the cloud environment.
* A Self-promoting attack might have been performed on cloud service sy, which means sx should have been selected instead.
* Disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks)
* Trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., Sybil attacks).

**PROPOSED SYSTEM:**

* Cloud service users’ feedback is a good source to assess the overall trustworthiness of cloud services. In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services.
* We introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place in a long or short period of time (i.e., strategic or occasional attacks respectively).
* We also develop an availability model that maintains the trust management service at a desired level. We also develop an availability model that maintains the trust management service at a desired level.

**ADVANTAGES OF PROPOSED SYSTEM:**

* TrustCloud framework for accountability and trust in cloud computing. In particular, TrustCloud consists of five layers including workflow,
* Propose a multi-faceted Trust Management (TM) system architecture for cloud computing to help the cloud service users to identify trustworthy cloud service providers.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : JAVA/J2EE
* IDE : Netbeans 7.4
* Database : MYSQL

**REFERENCE:**

Talal H. Noor, Quan Z. Sheng, *Member, IEEE,* Lina Yao, Schahram Dustdar, *Senior Member, IEEE,* and Anne H.H. Ngu, “CloudArmor: Supporting Reputation-based Trust Management for Cloud Services”, **IEEE Transactions on Parallel and Distributed Systems, 2015.**